Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (cancelled)

2. (previously presented) A method as described in claim 14 wherein said publicly known manner for deriving an integer from said published information comprises applying a hashing function to said message M.

3. (original) A method as described in claim 2 wherein said message M includes information IAV identifying said digital postage meter and operating parameters applicable to said digital postage meter.

4. (original) A method as described in claim 2 wherein said message M includes information IAV identifying said digital postage meter and operating parameters applicable to said digital postage meter.

5. (previously presented) A method as described in claim 14 wherein said group [P] is defined on an elliptic curve.

6. (previously presented) A method as described in claim 14 wherein said message M includes information tying said postage meter's public key Key_{DM}*P to said information IAV.

7. (cancelled)

8. (cancelled)

9. (cancelled)

10. (cancelled)

11. (cancelled)

12. (cancelled)

13. (cancelled)

14. (previously presented) A method for controlling, and distributing information between a digital postage meter and a certifying station operated by a certifying authority CA for publishing information, so that a public key $Key_{DM}*P$ of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from said published information with assurance that said public key $Key_{DM}*P$ has been certified by said certifying authority CA, said method comprising the steps of:

a) defining and publishing a finite group [P] with a binary operation [+] and publishing a particular point P in said group;

b) defining and publishing a binary operation K*p, where K is an integer and p is a point in said group, such that K*p is a point in said group computed by applying said operation [+] to K copies of said point p;

c) controlling a certifying station to publish a certificate OMC_{DM} for said digital postage meter, wherein;

$$OMC_{DM} = (r_{DM} + r_{CA})*P;\text{ and wherein}$$

r_{DM} is a random integer generated by said digital postage meter and r_{CA} is a random integer generated by said certifying station;

d) controlling said certifying station to publish a message M;

e) controlling said certifying station to generate an integer I_{DM} , and send said integer to said digital postage meter, wherein;

$I_{DM} = r_{CA} + H(M)Key_{CA;}$ and wherein

H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA;

f) publishing a public key $Key_{CA}*P$ for said certifying authority CA; and

g) controlling said digital postage meter to compute a private key Key_{DM},

$Key_{DM} = r_{DM} + I_{DM} = r_{DM} + r_{CA} + H(M)Key_{CA;}$ and

h) controlling said digital postage meter to print an indicium and digitally sign said indicium with said key Key_{DM}; whereby

i) said verifying party can compute said user's public key $Key_{DM}*P$ as

$Key_{DM}*P = OMC_{DM} + H(M)\ Key_{CA}*P =$

$(r_{DM} + r_{CA})*P + H(M)Key_{CA}*P$

from knowledge of H, M, [P], said public key $Key_{CA}*P$, and OMC_{DM}.

15. (previously presented) A method for controlling a digital postage meter to print indicia signed with a private key Key_{DM} based upon a published a finite group [P] with a binary operation [+] and a published particular point P in said group and a published a binary operation K*p, where K is an integer and p is a point in said group, such that K*p is a point in said group computed by applying said operation [+] to K copies of said point p, so that a public key $Key_{DM}*P$ of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from published information with assurance that said public key $Key_{DM}*P$ has been certified by a certifying authority CA, said method comprising the steps of:

a) controlling said digital postage meter to generate a random number r_{DM} and send a point r_{DM}*P to a certifying station;

b) controlling said digital postage meter to receive a certificate OMC_{DM} from a certifying station operated by said certifying authority CA, wherein;

$OMC_{DM} = (r_{DM} + r_{CA})$*P; and wherein

r_{DM} is a random integer generated by said digital postage meter and r_{CA} is a random integer generated by said certifying station;

c) controlling said digital postage meter to receive an integer I_{DM} from said certifying station, wherein;

$I_{DM} = r_{CA}+ H(M)Key_{CA}$; and wherein

M is a message published by said certifying station and H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA;

d) controlling said digital postage meter to compute a private key Key_{DM},

$Key_{DM} = r_{DM} + I_{DM} = r_{DM} + r_{CA}+ H(M)Key_{CA}$; and

e) controlling said digital postage meter to print an indicium and digitally sign said indicium with said key Key_{DM}; whereby

f) said verifying party can compute said digital postage meter public key Key_{DM}*P as

Key_{DM}*P = OMC_{DM} + H(M) Key_{CA}*P =

$(r_{DM} + r_{CA})$*P + H(M)Key_{CA}*P

from knowledge of H, M, [P], said public key Key_{CA}*P, and OMC_{DM}.

16. (previously presented) A method for controlling a certifying station operated by a certifying authority CA to publish information relating to a digital postage meter for

printing indicia signed with a private key Key_{DM} based upon a published a finite group [P] with a binary operation [+] and a published particular point P in said group and a published a binary operation K*P, where K is an integer and p is a point in said group, such that K*p is a point in said group computed by applying said operation [+] to K copies of said point p, so that a public key Key_{DM}*P of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from said published information with assurance that said public key Key_{DM}*P has been certified by a certifying authority CA, said method comprising the steps of:

a) controlling said certifying station to receive a point r_{DM}*P from said digital postage meter, where r_{DM} is a random number generated by said digital postage meter;

b) controlling said certifying station to generate and send to said digital postage meter a certificate OMC_{DM}, wherein;

$OMC_{DM} = (r_{DM} + r_{CA})*P$; and wherein

r_{CA} is a random integer generated by said certifying station;

c) controlling said certifying station to generate and send to said digital postage meter an integer I_{DM}, wherein;

$I_{DM} = r_{CA} + H(M)Key_{CA}$; and wherein

M is a message published by said certifying station and H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA; whereby

d) said digital postage meter can compute said private key Key_{DM},

$Key_{DM} = r_{DM} + I_{DM} = r_{DM} + r_{CA} + H(M)Key_{CA}$; and

and digitally sign said indicium with said key Key_{DM}; and whereby

e) said verifying party can compute said digital postage meter public key Key_{DM}*P as

$Key_{DM}*P = OMC_{DM} + H(M)\ Key_{CA}*P =$

$(r_{DM} + r_{CA})^{*}P + H(M)Key_{CA}{}^{*}P$

from knowledge of H, M, [P], said public key $Key_{CA}{}^{*}P$, and $CERT_{DM}$.

17. (previously presented) A method for controlling, and distributing information among a user station, a digital postage meter and a certifying station operated by a certifying authority CA for publishing information, so that a public key $Key_{50}{}^{*}P$ of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from said published information with assurance that said public key $Key_{50}{}^{*}P$ has been certified by said certifying authority CA, said method comprising the steps of:

a) defining and publishing a finite group [P] with a binary operation [+] and publishing a particular point P in said group;

b) defining and publishing a binary operation K*p, where K is an integer and p is a point in said group, such that K*p is a point in said group computed by applying said operation [+] to K copies of said point p;

c) controlling a certifying station to publish a certificate OMC_{50} for said digital postage meter, wherein;

$OMC_{50} = (r_{50} + r_{CA})^{*}P$; and wherein

r_{50} is a random Integer generated by said digital postage meter and r_{CA} is a random integer generated by said certifying station;

d) controlling said certifying station to publish a message M;

e) controlling said certifying station to generate an integer I_{50} , and send said integer to said user station , wherein;

$I_{50} = r_{CA} + H(M)Key_{CA}$; and wherein

H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA;

f) publishing a public key Key_{CA}*P for said certifying authority CA; and

g) controlling said user station to compute a private key Key_{50},

$Key_{50} = r_{50} + l_{50} = r_{50} + r_{CA} + H(M)Key_{CA;}$ and

h) transmitting said key Key_{50} to said postage meter; whereby

i) said digital postage meter can print an indicium and digitally sign said indicium with said key Key_{50}; and whereby

i) said verifying party can compute said user's public key Key_{50}*P as

$Key_{50}{*}P = OMC_{50} + H(M)\ Key_{CA}{*}P =$

$(r_{50} + r_{CA}){*}P + H(M)Key_{CA}{*}P$

from knowledge of H, M, [P], said public key Key_{CA}*P, and OMC_{50}.

18. (previously presented) A method as described in claim 17 wherein said publicly known manner for deriving an integer from said published information comprises applying a hashing function to said message M.

19. (previously presented) A method as described in claim 18 wherein said message M includes information IAV identifying said digital postage meter and operating parameters applicable to said digital postage meter.

20. (previously presented) A method as described in claim 17 wherein said message M includes information IAV identifying said digital postage meter and operating parameters applicable to said digital postage meter.

21. (previously presented) A method as described in claim 17 wherein said group [P] is defined on an elliptic curve.

22. (previously presented) A method as described in claim 17 wherein said message M includes information tying said postage meter's public key $Key_{50}*P$ to said information IAV.

23. (previously presented) A method for controlling a certifying station operated by a certifying authority CA to publish information relating to a digital postage meter for printing indicia signed with a private key Key_{50} based upon a published a finite group [P] with a binary operation [+] and a published particular point P in said group and a published a binary operation K*p, where K is an integer and p is a point in said group, such that K*p is a point in said group computed by applying said operation [+] to K copies of said point p, so that a public key $Key_{DM}*P$ of said digital postage meter can be determined by a party seeking to verify indicia printed by said digital postage meter from said published information with assurance that said public key $Key_{DM}*P$ has been certified by a certifying authority CA, said method comprising the steps of:

a) controlling said certifying station to receive a point $r_{DM}*P$ from a user station, where r_{DM} is a random number generated by said user station;

b) controlling said certifying station to generate and send to said user station a certificate OMC_{50}, wherein;

$OMC_{50} = (r_{50} + r_{CA})*P$; and wherein

r_{CA} is a random integer generated by said certifying station;

c) controlling said certifying station to generate and send to said user station an integer I_{50}, wherein;

$I_{50} = r_{CA} + H(M)Key_{CA}$; and wherein

M is a message published by said certifying station and H(M) is an integer derived from said message M in accordance with a publicly known algorithm H and Key_{CA} is a private key of said certifying authority CA; whereby

d) said user station can compute said private key Key_{DM},

$$Key_{50} = r_{50} + l_{50} = r_{50} + r_{CA} + H(M)Key_{CA}$$

and transmit said key Key_{50} to said digital postage meter; whereby

e) said digital postage meter can digitally sign said indicium with said key Key_{50}; and whereby

f) said verifying party can compute said digital postage meter public key Key_{50}*P as

$$Key_{50}{}^*P = OMC_{50} + H(M)\ Key_{CA}{}^*P =$$
$$(r_{DM} + r_{CA}){}^*P + H(M)Key_{CA}{}^*P$$

from knowledge of H, M, [P], said public key Key_{CA}*P, and $CERT_{DM}$.

24. (previously presented) A method for determining a public key Key_{DM}*P of a digital postage meter with assurance that said key Key_{DM} has been certified by a group of one or more certifying authorities CA, said method comprising the steps of:

a) scanning an indicium produced by said postage meter to obtain a certificate OMC_{DM} for said postage meter, wherein;

$OMC_{DM} = (r_{DM} + sum(r_{CAi})){}^*P$; and wherein

r_{DM} is a random integer known only to a party generating said key Key_{DM} and $sum(r_{CAi})$ is a sum of a plurality of random integers r_{CAi}, an ith one of said certifying stations generating an ith one of said random integers r_{CAi};

b) scanning said indicium produced by said postage meter to obtain a message M said message M being published by a certifying station operated by one of said certifying authorities CA;

c) computing a hash H(M) of said message M in accordance with a predetermined hashing function H;

d) obtaining at least one public key $_{CAi}$*P corresponding to said one or more certifying authorities CA, an ith one of said authorities having an ith one of said keys Key$_{CAi;}$ and

e) computing said user's public key Key$_U$*P as

$$\mathrm{Key}_U{*}P = \mathrm{CERT}_U\,[+]\ H(M)\mathrm{sum}_{[+]}(\mathrm{KeyCAi}{*}P\ )=$$
$$(r_U + \mathrm{sum}(r_{CAi})){*}P\ [+]\ \mathrm{sum}(H(M)\mathrm{Key}_{CAi}){*}P;$$ wherein

f) a binary operation [+] is defined on a finite group [P] having a published particular point P; and

g) K*p, is a second binary operation defined on said group [P], where K is an integer and p is a point in said group, such that K*p, is a point in said group computed by applying said operation [+] to K copies of said point p.

25. (canceled)

26. (canceled)

27. (previously presented) A method as described in claim 31 wherein M = (e,IAV), where IAV is an identity and attributes value for said postage meter.

28. (canceled)

29. (canceled)

30. (previously presented) A method as described in claim 32 wherein M = (e,IAV), where IAV is an identity and attributes value for said postage meter.

31. (previously presented) A method of digitally signing a postal indicium comprising the steps of:

a) generating a message m, said message m including indicia data;

b) generating a digital signature with message recovery for said message m; and

c) incorporating said digital signature into said indicium; wherein

d) said generating step further comprises the substeps of:

d1) generating a random integer r_S, $r_S < n$, where n is the order of a group [P] defined on an elliptic curve;

d2) generating a integer K,

$K= K(r_S{*}P)$

where K(p) is a mapping of points in [P] onto the integers, and P is a particular published point in [P];

d3) generating e,

$e = SKE_K(m)$

where SKE_K is a symmetric key encryption algorithm using key K;

d4) generating H(M), where H is a hashing function and M is a message which can be recovered from said indicium;

d5) generating $s = Key_{DM}H(M) + r_S$,

where Key_{DM} is the private key of a postage meter which produced said indicium; and

d6) setting said digital signature for said message m equal to the pair (s,e).

32. (previously presented) A method of verifying a digital signature of a postal indicium comprising the steps of:

a) recovering a message m from a digital signature of a postal indicium; and

b) accepting said signature as valid if said message m is internally consistent; wherein

c) said recovering step further comprises the substeps of:

c1) recovering a public key $Key_{DM}*P$ for a postage meter which produced said indicium;

c2) obtaining the signature (s,e) of said indicium, where $s = Key_{DM}H(M) +r_S$ and $e = SKE_K(m)$, where SKE_K is a symetric key encryption algorithm using key K, m is indicia data, and M is a message recoverable from said indicium;

c3) obtaining M from said indicium;

c4) generating

$$s*P\ [-]\ H(M)Key_{DM}*P =$$
$$H(M)Key_{DM}*P\ [+]\ r_S*P\ [-]\ H(M)Key_{DM}*P =$$
$$r_S*P$$

where [-] is the inverse of [+];

c5) generating

$$K = K(r_S*P)$$

where K(p) is a mapping of points in [P] onto the integers, and P is a particular published point in [P];

c6) generating

$$m = SKE^{-1}_K(e)$$

where SKE^{-1}_K is the inverse of SKE_K.